МІЖНАРОДНО-ПОЛІТИЧНІ ВИМІРИ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2024. – Т. 50. – С. 9-19
DOI: 10.31861/mhpi2024.50.9-19

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2024. – Volume. 50. – pp. 9-19
DOI: 10.31861/mhpi2024.50.9-19

УДК 327:004.738.5(477)

© Оксана Вознюк [1]

Інформаційна війна як інструмент міжнародної політики (досвід для України)

У статті розглядається інформаційна війна як інструмент міжнародної політики на прикладі сучасної України. Актуальність теми зумовлена тим, що інформаційна війна стала невід'ємною частиною гібридних конфліктів у світі, і її вплив на міжнародні відносини, внутрішню політику держав, а також на громадську думку постійно зростає. Україна, яка є об'єктом тривалих інформаційних атак із боку Росії, накопичила важливий досвід, що може бути корисним для інших держав у контексті протидії інформаційним загрозам. Результати дослідження показали, що Росія активно використовує широкий арсенал інформаційних інструментів, таких як дезінформація, пропаганда, маніпуляція історичними фактами та кібероперації. Україна, своєю чергою, вдало інтегрує міжнародну співпрацю та власні стратегії для протидії цим загрозам, використовуючи досвід інших країн і міжнародні ініціативи. Розробка національних стратегій, заснованих на міжнародному досвіді, та впровадження нових підходів до протидії інформаційним атакам є ключовими факторами успішної боротьби з сучасними інформаційними загрозами.

Ключові слова: гібридна війна, інформаційна політика, інформаційна безпека, дезінформація, концепція «м'якої сили».

Information Warfare as a Tool of International Policy (Experience for Ukraine)

The article examines the role of information warfare as a tool of international politics, with a special emphasis on the experience of Ukraine in the conditions of the modern hybrid conflict with Russia. The topicality of the topic is determined by the fact that information warfare is one of the main components of modern military-political conflicts, where information is used to undermine state institutions, discredit the authorities, manipulate public opinion and destabilize societies. The purpose of the study is to study scientific approaches to the analysis of information warfare, to identify key tools and technologies used in information operations against Ukraine, as well as to assess the importance of international cooperation and support in strengthening the state's resilience to information threats. Research methods included the analysis of scientific sources, publications, analytical reports and specific information operations directed against Ukraine. The methods of content analysis were used to study information narratives that spread through different channels, a systematic approach to assess the complex impact of information attacks on the state, as well as a comparative analysis to identify similar and different strategies of information warfare in other countries. The results of the study showed that Russia uses a wide arsenal of information technologies, such as the spread of fake news, manipulation of historical facts, active use of social media and cyber operations. These actions are aimed not only at destabilizing Ukraine, but also at the international audience in order to spread pro-Russian narratives. In addition, the study found that the international community plays an important role in supporting Ukraine by providing technical, financial and expert assistance. International initiatives and

[1] Кандидат педагогічних наук, доцент, професор кафедри воєнної історії Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, Україна. E-mail: voznuko206@gmail.com; https://orcid.org/ 0000-0002-4186-6113.

coalitions aimed at combating disinformation have become an important element of ensuring information security in Ukraine. The conclusions emphasize that effective countermeasures against information warfare require a comprehensive approach that includes cooperation between government institutions, public organizations, the private sector, and international partners.

Keywords: hybrid war, information policy, information security, disinformation, concept of «soft power».

Постановка наукової проблеми та її значення. Інформаційна війна є основним компонентом сучасних гібридних конфліктів, у яких інформація використовується як стратегічний ресурс для досягнення політичних, економічних та військових цілей. Її значення виходить далеко за межі традиційної пропаганди або дезінформації, охоплюючи складні механізми впливу на суспільну свідомість, політичні процеси, економічні системи й міжнародні відносини. Для України, яка перебуває на передовій інформаційного протистояння, особливо з Росією, критично важливим є поглиблене розуміння природи інформаційної війни.

Особливої уваги потребує концептуалізація сучасних підходів до визначення інформаційної війни. Які саме методи, інструменти та форми інформаційної агресії використовуються у глобальних конфліктах? Чи є виявлені в наукових колах характеристики інформаційної війни достатніми для створення дієвої архітектури інформаційної безпеки? Відсутність єдиного розуміння цих питань ускладнює формування стратегій протидії.

Російська інформаційна війна є багатошаровим явищем, що охоплює маніпуляції суспільною думкою через соціальні мережі, створення деструктивних наративів, дискредитацію державних інституцій та втручання в міжнародний інформаційний простір. Ці аспекти недостатньо досліджені з погляду їхнього впливу на глобальні інформаційні процеси, що створює прогалини у спроможності України ефективно протидіяти таким загрозам.

Актуальність вивчення проблеми полягає у формуванні нових підходів до аналізу й нейтралізації інформаційної агресії. Це дослідження спрямоване на розробку наукових основ для розуміння інформаційної війни як явища та створення ефективної національної інформаційної стратегії.

Отже, дослідження інформаційної війни дасть змогу не лише вдосконалити систему протидії сучасним загрозам, але й створити передумови для побудови нової архітектури інформаційної безпеки, яка базуватиметься на науково обґрунтованих підходах.

Аналіз останніх досліджень і публікацій. Інформаційна війна в контексті конфлікту на сході України була предметом наукової уваги значної кількості українських дослідників. Зокрема, М. В. Білоусов, В. Г. Алєйник[2] висвітлюють специфіку російських інформаційних операцій проти України. Учені вказують на те, що Росія використовує багаторівневі дезінформаційні кампанії для впливу на внутрішню та міжнародну аудиторію, які спрямовані на дискредитацію української влади та розкол суспільства. Автори підкреслюють важливість міжнародної підтримки та співпраці для ефективної протидії таким загрозам. Не менш важливим є дослідження І. М. Сопілко[3], яка докладно описує методи, що використовуються для маніпуляції масовою свідомістю в умовах постправди. Науковиця звертає увагу на те, як новітні медіа та соціальні мережі стають ключовими майданчиками для ведення інформаційної війни. Учена акцентує на тому, що традиційні методи боротьби з дезінформацією стають менш ефективними, тому державам необхідно розробляти нові підходи та стратегії.

І. Й. Краснодемська [4] аналізує стратегії протидії російським інформаційним операціям. Зокрема, дослідниця наголошує на необхідності більш активного використання інструментів публічної дипломатії та медіаграмотності населення для зміцнення інформаційної безпеки. Ав-

[2] Білоусов, М. В., Алєйник, В. Г. (2023). Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки. *Регіональні студії.* № 33. С. 119–125. DOI https://doi.org/10.32782/2663-6170/2023.33.18.

[3] Сопілко, І. М. (2022). Інформаційна війна проти України та правові засоби протидії злочинним засобам. *Юридичний вісник*. № 3 (64). С. 108–115. DOI: 10.18372/2307-9061.64.16897.

[4] Краснодемська, І. Й. (2021). Окупація Криму Російською Федерацією в контексті геополітичної парадигми початку XXI ст. *Всеукраїнська науково-практичної конференція «Соціально-політичні процеси в Україні та світі у контексті глобалізаційних перетворень», 23 квітня 2021 року.* Ірпінь: Університет ДФС України. С. 81–90.

торка доводить, що успішна протидія дезінформації вимагає комплексного підходу, який поєднує державні, громадські та приватні зусилля.

У західній науковій літературі інформаційна війна також розглядається як багатоаспектне явище. Наприклад, J. Kiera[5] досліджує роль пропаганди та маніпуляцій у формуванні громадської думки через медіа та соціальні платформи. Він акцентує на тому, як авторитарні режими використовують інформаційні інструменти для посилення контролю над суспільством.

V. Stumbrus[6] пропонує концепцію превентивного підходу до протидії інформаційній війні, наголошуючи на важливості запобігання поширенню дезінформації шляхом посилення прозорості державних інститутів і створення механізмів перевірки фактів.

Сучасні тенденції в зарубіжній науці також охоплюють дослідження феномену «deepfake» та автоматизованого поширення дезінформації через бот-мережі, що аналізуються, зокрема, у роботах R. Szpyra[7]. Автор підкреслює, що швидке поширення технологій вимагає постійного оновлення інструментів захисту інформаційного простору.

Західні дослідники часто розрізняють два явища: запобігання (превенція) інформаційній війні та активна протидія їй. Превентивні заходи передбачають розвиток медіаграмотності, підвищення рівня критичного мислення серед населення та зміцнення демократичних інститутів. Водночас протидія передбачає оперативне виявлення дезінформації, її нейтралізацію та інформування громадськості про загрози.

Отже, сучасні наукові розвідки в галузі інформаційної війни як в Україні, так і за кордоном, підкреслюють важливість розвитку системного підходу до забезпечення інформаційної безпеки. Інтеграція українського та західного досвіду дозволяє сформувати більш ефективну архітектуру протидії дезінформаційним загрозам.

Метою статті є дослідження інформаційної війни як інструменту міжнародної політики та аналіз її впливу на Україну в контексті сучасних геополітичних реалій. Стаття спрямована на виявлення основних стратегій та методів інформаційної агресії, зокрема з боку Росії, а також визначення ефективних механізмів протидії цим загрозам для зміцнення інформаційної безпеки України. Основними завданнями нашої наукової розвідки є: 1) здійснити огляд наукових підходів до вивчення інформаційної війни в контексті міжнародних відносин та її місця в сучасній політиці; 2) визначити ключові інструменти та технології, які використовуються в інформаційній війні проти України; 3) оцінити роль міжнародної співпраці та підтримки в зміцненні інформаційної стійкості України.

Виклад основного матеріалу. Інформаційна війна є складним і багатогранним феноменом, що викликає зацікавленість науковців із різних сфер, зокрема міжнародних відносин, комунікаційних наук та безпекових досліджень. Існує кілька основних підходів до аналізу цього явища, кожен з яких надає унікальну перспективу для розуміння сутності та наслідків інформаційних конфліктів. Огляд основних підходів до визначення сутності інформаційної війни представлено в *таблиці 1.*

У процесі дослідження було критично оцінено всі представлені підходи. Кожен із них пропонує важливий аналітичний інструментарій, але жоден не може повністю охопити всю складність і багатогранність явища інформаційної війни. Наприклад, стратегічний підхід наголошує на інтеграції інформаційної війни до ширших гібридних стратегій, але недостатньо враховує вплив когнітивних процесів і технологічних аспектів.

Водночас когнітивний підхід акцентує на психологічних аспектах, проте може ігнорувати глобальний контекст і технічні засоби поширення інформації. Комунікаційний і системний підходи розглядають технологічні й глобальні аспекти, але не завжди враховують вплив на індивідуальному та суспільному рівнях.

Автор цієї статті пропонує інтегративний підхід, який поєднує елементи когнітивного, комунікаційного та системного підходів. Такий підхід дає змогу аналізувати інформаційну війну як багаторівневий процес, що охоплює як індивідуальні когнітивні механізми, так і вплив

[5] Kiera, J. (2022). Information warfare as a foreign policy tool of the russian federation. *No Limits.* Vol. 2(6), 30-31. DOI: https://doi.org/10.31261/no_limits.2022.6.09.

[6] Stumbrus, V. (2024). Some elements of defining information warfare. *Public security and public order.* Vol. 35. P. 284-295. DOI: 10.13165/PSPO-24-35-21.

[7] Szpyra, R. (2020). Russian information offensive in the international relations. *Security and Defence Quarterly.* Vol. 30. P. 31-47. DOI: http://doi.org/10.35467/sdq/124436.

Таблиця 1

Огляд основних підходів до аналізу інформаційної війни

Стратегічний підхід
Інформаційна війна розглядається як частина ширшої стратегії гібридної війни. Цей підхід базується на тому, що інформаційна війна використовується разом з іншими формами впливу, такими як економічні санкції, дипломатичний тиск і військові операції. Головна мета таких дій полягає в тому, щоб послабити суперника без необхідності прямого застосування сили. У цьому контексті інформаційні операції використовуються для дезорієнтації, деморалізації та створення хаосу в суспільстві, що є ключовими елементами сучасних конфліктів.
Когнітивний підхід
Зосереджений на дослідженні психологічних і соціальних механізмів, які лежать в основі сприйняття інформації. Цей підхід наголошує на тому, що інформаційні війни ведуться не тільки через поширення фейкових новин, але й через маніпуляцію уявленнями, переконаннями та емоціями людей. Метою є вплив на свідомість цільової аудиторії, формування її світогляду та зміна поведінкових реакцій. Цей підхід дозволяє досліджувати, як інформація, навіть якщо вона є правдивою, може бути використана для маніпуляцій.
Комунікаційний підхід
Аналізує, яким чином інформація передається й поширюється через різні канали, зокрема соціальні медіа, телебачення, друковані ЗМІ та інтернет-ресурси. Він підкреслює роль технологій у сучасній інформаційній війні, особливо в еру цифрових технологій, коли інформація може поширюватися миттєво й охоплювати великі аудиторії. Цей підхід також досліджує феномен «інформаційних бульбашок», коли люди споживають інформацію, яка підтверджує їхні вже наявні переконання, що підсилює ефект пропаганди.
Системний підхід
Аналізує інформаційну війну як частину глобальної системи взаємодії держав і недержавних гравців. Важливою складовою цього підходу є розуміння того, як інформаційні операції впливають на політичну, економічну та соціальну стабільність країн, як вони можуть бути використані для досягнення стратегічних цілей на міжнародній арені. Інформаційні атаки часто мають глобальні наслідки, створюючи виклики не лише для окремих держав, але й для міжнародної спільноти загалом.

Джерело: складено на основі Стадник, А. Г. (2015). Основні моделі організації інформаційних війн та їх різновиди. *Соціальні технології: актуальні проблеми теорії та практики.* Вип. 67–68. С. 81–91. Режим доступу: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf.

на глобальну політику та міжнародні відносини. Це забезпечує цілісне розуміння інформаційної війни та створює основу для розроблення ефективних механізмів протидії.

Варто зауважити, що саме інформаційна війна використовується як частина гібридної війни, що стала однією з найпоширеніших форм сучасних конфліктів. Гібридна війна поєднує традиційні воєнні дії з невоєнними засобами, такими як політичний тиск, економічні санкції, кібернетичні атаки та, найголовніше, інформаційна агресія. Саме інформаційна війна відіграє ключову роль у гібридних конфліктах, оскільки дозволяє впливати на свідомість населення, маніпулювати громадською думкою та дестабілізувати внутрішньополітичну ситуацію в країні-цілі [8].

У гібридній війні інформаційні атаки починаються задовго до того, як конфлікт набуває військового характеру. Спочатку ворог використовує пропаганду та дезінформацію для створення сприятливих умов для подальших агресивних дій. Наприклад, це може бути поширення неправдивих наративів про політичну нестабільність, економічні проблеми або міжетнічні конфлікти в країні-цілі. Такий підхід дозволяє посіяти сумніви в здатності держави ефективно функціонувати, тим самим підриваючи довіру громадян до власної влади.

[8] Коруц, У. (2020). Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Підприємництво, господарство і право.* №8. DOI https://doi.org/10.32849/2663-5313/2020.8.55.

Окрім цього, інформаційна війна в гібридному конфлікті спрямована на деморалізацію населення та зниження бойового духу військових. З цією метою використовуються спеціально підготовлені фейкові новини, які поширюються через соціальні мережі, новинні ресурси або навіть локальні медіа. Ці повідомлення можуть мати різноманітний характер: від перебільшених втрат на полі бою до вигаданих історій про корупцію чи зраду серед військових та політичних лідерів[9].

Також важливо зазначити, що інформаційна війна в межах гібридного конфлікту має на меті не лише атакувати країну-ціль, але й формувати позитивний образ агресора. Це досягається через так звану «м'яку силу» – створення наративів, що виправдовують агресію, представляючи її як захист певних груп населення, забезпечення стабільності чи відновлення історичної справедливості. Така інформаційна стратегія дозволяє агресору зберігати позитивний імідж як на міжнародній арені, так і серед власного населення.

Інформаційна війна також використовується для маскування реальних намірів агресора. Через постійний потік дезінформації створюється інформаційний шум, у якому стає складніше відрізнити правду від неправди. Це ускладнює реакцію міжнародної спільноти та підготовку до відповіді на агресію, оскільки поки триває аналіз ситуації, агресор встигає досягти своїх стратегічних цілей.

Зважаючи на складність гібридних конфліктів, інформаційна війна стає критично важливою зброєю. Її роль не можна недооцінювати, оскільки інформаційні атаки впливають не лише на військову складову, а й на соціальну, політичну та економічну стабільність держав. Саме тому ефективна протидія інформаційним загрозам є важливою частиною сучасної стратегії національної безпеки будь-якої держави, зокрема й України, яка вже багато років перебуває в епіцентрі гібридної війни.

Інформаційна війна як частина гібридної стратегії розгорнулася проти України задовго до відкритого військового вторгнення. Передумови для цього можна було спостерігати ще з моменту проголошення незалежності України в 1991 році. Від самого початку Росія активно використовувала інформаційний вплив для підриву політичної стабільності та національної ідентичності України. Інформаційні атаки, спрямовані на дискредитацію української державності, культивували в суспільстві думку про те, що Україна є «незрілою» державою, залежною від Росії.

Перші кроки цієї кампанії можна віднести до періоду після Помаранчевої революції 2004 року, коли стало зрозуміло, що Україна рухається до євроінтеграції, а не в бік зближення з Росією. Саме тоді почали посилюватися російські інформаційні операції, спрямовані на дискредитацію українських політичних лідерів, зокрема тих, хто підтримував проєвропейський курс. ЗМІ, контрольовані Росією, активно поширювали дезінформацію, намагаючись посіяти розбрат у суспільстві та викликати сумніви в правильності вибраного вектору розвитку[10].

Після Революції Гідності у 2014 році, яка стала переломним моментом в українській історії, інформаційна війна набула нових масштабів. Анексія Криму та розпалювання війни на Донбасі супроводжувалися масовими інформаційними атаками. Російські медіа розпочали активну кампанію з поширення пропагандистських матеріалів, наративів про «фашизм» в Україні, необхідність «захисту російськомовного населення» та спроби представити Майдан як результат іноземного втручання. Одним із перших і найбільш помітних кроків було створення уявлення про «громадянську війну» в Україні, що мало на меті дезорієнтувати міжнародну спільноту та виправдати агресивні дії Росії.

Особливо активним інструментом стала дезінформація, яка поширювалася через різні канали: від традиційних ЗМІ до соціальних мереж. Дезінформаційні кампанії часто поєднувалися з кібернетичними атаками, спрямованими на порушення роботи урядових інституцій, руйнування довіри до українських ЗМІ та створення хаосу в суспільстві. Важливо зазначити, що мета

[9] Галіпчак, В. (2023). Інформаційна війна як складова гібридної війни в умовах російської агресії. *Вісник Прикарпатського університету. Серія: Політологія.* № 15 (1). С. 26–32. DOI: https://doi.org/10.32782/2312-1815/2024-1-4.

[10] Сащук, Г. М., Рихлік, В. А. (2022). Інформаційний складник гібридної війни Росії проти України. *Політологічний вісник КНУ ім. Т. Шевченка.* № 89. С. 133–146. DOI: 10.17721/2415–88IX.2022.89.133-146.

цих атак не лише дискредитувати українську владу, а й деморалізувати населення, змусити людей сумніватися у власних силах та майбутньому країни.

Водночас Росія активно використовувала концепцію так званої «м'якої сили» для зміцнення своїх позицій в інформаційному просторі. Важливу роль у цьому процесі відігравали російськомовні телеканали, які продовжували транслюватися в Україні навіть після початку збройного конфлікту. Вони виконували роль своєрідних рупорів пропаганди, через які насаджувалися проросійські наративи, що мали на меті посіяти розбрат між різними регіонами країни, відновити колишню залежність від Росії та зруйнувати єдність українського суспільства.

Після перших кроків у межах інформаційної війни, спрямованих на підготовку суспільної думки як в Україні, так і за її межами, російські інформаційні операції перейшли в нову, більш інтенсивну фазу під час відкритого військового конфлікту. У цьому контексті дезінформація та пропаганда стали потужними інструментами гібридної війни, що супроводжували військову агресію. Російські медіаресурси, соціальні мережі та інші платформи активно використовувалися для формування викривленого уявлення про події, дискредитації українського уряду та збройних сил, а також для деморалізації населення[11].

Один з яскравих прикладів російських інформаційних операцій можна помітити під час анексії Криму у 2014 році. Кремлівські ЗМІ поширювали наратив про те, що на півострові відбувся «мирний референдум» за бажанням місцевого населення, тоді як насправді це було силове захоплення території, яке супроводжувалося присутністю російських військових без розпізнавальних знаків. Водночас російська пропаганда активно працювала над дискредитацією української влади, стверджуючи, що новий уряд у Києві є нелегітимним і захопив владу шляхом перевороту[12].

Ще одним вагомим прикладом є війна на Донбасі, де інформаційна війна йшла паралельно з військовими діями. З самого початку конфлікту російські ЗМІ намагалися переконати аудиторію як у Росії, так і за її межами, що на сході України йде «громадянська війна», а не російська агресія. Наративи про «фашистів у Києві», які нібито переслідують російськомовне населення, стали основою пропаганди, щоб виправдати дії проросійських бойовиків та військову підтримку з боку Росії. Водночас будь-які українські військові операції для відновлення контролю над своєю територією зображувалися як агресивні дії проти мирних жителів Донбасу[13].

Російські інформаційні атаки були також спрямовані на підрив довіри до західних партнерів України. Наприклад, у 2014–2015 роках, коли Захід запровадив санкції проти Росії через агресію в Україні, російські ЗМІ почали активну кампанію з дискредитації цих заходів. Пропагандисти стверджували, що санкції не впливають на економіку Росії, а є лише символічним жестом, і водночас поширювали дезінформацію про те, що ці санкції шкодять самим західним країнам більше, ніж Росії.

Соціальні мережі також стали полем для масових інформаційних операцій. За даними досліджень, російські «тролі» та боти активно працювали для поширення фейкових новин, які мали на меті дискредитувати українське керівництво та армію. Вони створювали сотні акаунтів у соціальних мережах для того, щоб поширювати дезінформацію, викликати паніку серед населення або маніпулювати суспільною думкою на міжнародному рівні. Одним із найбільш відомих випадків стала кампанія з дезінформацією щодо трагедії рейсу MH17, збитого над територією Донбасу в липні 2014 року. Російські ЗМІ та інтернет-ресурси намагалися перекла-

[11] Грицай, Р. О. (2023). Інформаційні війни: пошук стратегій протидії. *Публічне управління і адміністрування в Україні*. Вип. 33. С. 18–23. Режим доступу: https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf (дата звернення: 03.10.2024).

[12] Денисяка, О. (2024). Росія успішно просуває свої наративи про Україну у західних ЗМІ. *Голос Америки. Львівський портал*. [онлайн]. Режим доступу: https://portal.lviv.ua/news/2024/06/30/rosiia-uspishno-prosuvaie-svoi-naratyvy-pro-ukrainu-u-zakhidnykh-zmi-holos-ameryky (дата звернення: 03.10.2024).

[13] Тимошенко, Д. (2024). Від танків «з воєнторгу» до наступу на Київ: чому Захід 10 років боявся назвати РФ агресором. *Радіо Свобода.* [онлайн]. Режим доступу: https://www.radiosvoboda.org/a/viyna-rosiyi-proty-ukrayiny-vyznachennya/32826392.html (дата звернення: 03.10.2024).

сти провину за збиття літака на Україну, поширюючи фейкові версії подій, хоча міжнародне розслідування довело, що літак був збитий російською ракетою[14].

Ще однією тактикою Росії була зміна фокуса уваги міжнародної спільноти. Важливі політичні події, такі як вибори в Україні чи військові операції ЗСУ, супроводжувалися хвилями дезінформації або провокацій, спрямованими на відвертання уваги громадськості від справжньої ситуації на місцях.

Ці реальні приклади демонструють, наскільки потужними є інформаційні операції в руках держави, яка використовує їх для досягнення стратегічних цілей. Україні важливо навчитися ефективно протидіяти таким загрозам, оскільки інформаційна війна залишається однією з ключових складових сучасної гібридної агресії, здатної впливати на внутрішню стабільність та міжнародну репутацію країни.

Після того, як стало зрозуміло, що Росія активно використовує інформаційну війну як важливий інструмент для дестабілізації ситуації в Україні, державні інституції почали вживати заходів для захисту національного інформаційного простору.

Одним із перших важливих кроків стало посилення державного регулювання медіапростору. У 2014 році Україна ухвалила низку постанов, які передбачали блокування доступу до російських пропагандистських телеканалів, що поширювали фейки про події в Україні та виправдовували російську агресію. Було також введено заборону на поширення певних російських ЗМІ, що активно використовувалися для маніпуляції громадською думкою. Це рішення дало змогу обмежити доступ до відверто пропагандистських джерел, які намагалися впливати на населення як в Україні, так і за її межами[15].

Другий важливий напрям – це активна робота українських спецслужб у сфері кібербезпеки. Кібератаки стали частиною російських інформаційних операцій, особливо в критичні моменти, зокрема під час виборів або військових операцій. Україна розробила стратегії захисту від таких атак, створивши національні органи для кібербезпеки, які займаються моніторингом та протидією спробам зламати державні інформаційні системи. Одним із прикладів була масштабна кібератака на енергетичну інфраструктуру України у 2015 році, яку вдалося відбити завдяки швидким діям і посиленій співпраці з міжнародними партнерами.

Україна також активно почала використовувати можливості цифрової дипломатії та інформування міжнародної спільноти. У межах цієї стратегії була запроваджена низка ініціатив, спрямованих на покращення міжнародного розуміння реальної ситуації в Україні. Міністерство зовнішніх справ України та інші державні органи почали активніше взаємодіяти з міжнародними журналістами й медіа для спростування фейкових новин, поширених російськими пропагандистами. Це сприяло формуванню більш адекватної картини подій в очах міжнародної аудиторії, що стало важливим інструментом у боротьбі за підтримку України на світовій арені[16].

Окрему увагу варто приділити розвитку українських незалежних медіа та суспільних організацій, які відіграють значну роль у протидії російській дезінформації. Створення таких платформ, як «СтопФейк», дало змогу виявляти та спростовувати пропагандистські наративи. Такі ініціативи не лише підвищують рівень медіаграмотності серед населення, але й допомагають у спростуванні фейкових новин, що поширюються ворогом[17].

Важливо зазначити роль міжнародної підтримки в посиленні українського інформаційного захисту. Україна активно співпрацює з Європейським Союзом та іншими партнерами для

[14] Десять років з моменту трагедії рейсу MH17: пам'ять та правда (2024). *Електронне видання Еспресо*. [онлайн]. Режим доступу: https://espreso.tv/news-desyat-rokiv-z-momentu-tragedii-reysu-mh17-pamyat-ta-pravda (дата звернення: 03.10.2024).

[15] Коріновська, Н., Грейс, М. (2017). Порошенко підписав указ про заборону «ВКонтакте» і Mail.ru в Україні. *Hromadske.* [онлайн]. Режим доступу: https://hromadske.ua/posts/prezydent-ukrainy-petro-poroshenko-pidpysav-ukaz-pro-novi-sanktsii (дата звернення: 03.10.2024).

[16] Феськов, І. В. (2016). Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики.* Вип. 58. С. 66–77. Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/622a115c-5b8a-4cd3-8bf9-a87c614b3e66/content (дата звернення: 03.10.2024).

[17] Загурська-Антонюк, В. Ф. (2020). Політично-інформаційні безпекові механізми в українській державній системі у контексті геополітичних змін. *Державне управління: удосконалення та розвиток.* №2. Режим доступу: http://nbuv.gov.ua/UJRN/Duur_2020_2_10 (дата звернення: 03.10.2024).

зміцнення своїх можливостей у сфері інформаційної безпеки. Західні країни надають технічну, консультативну й фінансову підтримку для розвитку інструментів протидії інформаційним атакам, що дозволяє Україні бути більш підготовленою до нових викликів.

Україна, захищаючи свій інформаційний простір, активно вивчає міжнародний досвід у боротьбі з дезінформацією. Багато країн та міжнародних організацій уже напрацювали ефективні моделі та стратегії, які демонструють успіх у протидії інформаційним загрозам. Приклади таких ініціатив можуть стати корисними як для посилення внутрішніх механізмів захисту, так і для міжнародної співпраці.

Однією з найуспішніших ініціатив є створення East StratCom Task Force – спеціальної групи Європейського Союзу, що займається моніторингом та боротьбою з дезінформацією, насамперед з боку Росії. Група була створена у 2015 році у відповідь на посилення інформаційних загроз в Європі. Її головною метою є виявлення неправдивих новин, спростування фейкових повідомлень та поширення перевіреної інформації. Через свою платформу EU vs Disinfo організація публікує звіти, що містять приклади маніпуляцій та дезінформаційних кампаній, надаючи користувачам інструменти для виявлення неправдивої інформації. Завдяки постійній роботі ця ініціатива допомогла знизити рівень впливу пропаганди та підвищити медіаграмотність європейської спільноти[18].

Ще одним прикладом успішної міжнародної ініціативи є програма НАТО щодо стратегічних комунікацій (NATO StratCom), яка спрямована на протидію дезінформації та підтримку союзників у боротьбі з інформаційними атаками. Ця ініціатива фокусується не тільки на спростуванні фейків, але й на просуванні позитивних наративів, які допомагають захищати демократичні цінності та зміцнювати міжнародну стабільність. Важливим елементом цієї програми є взаємодія з національними урядами та медіа, що дозволяє створювати стійкіші інформаційні простори[19].

Важливим для України є досвід скандинавських країн, зокрема Фінляндії, яка системно працює над підвищенням медіаграмотності свого населення. Фінська модель передбачає навчальні програми в школах, де учнів навчають розпізнавати фейки та критично аналізувати інформацію, отриману з медіа. Цей підхід дозволив значно знизити рівень впливу дезінформації та зробив населення більш стійким до зовнішніх інформаційних загроз. Досвід Фінляндії може стати зразком для країн, що стикаються з подібними викликами, зокрема для України, де медіаграмотність також стає ключовим елементом інформаційної безпеки[20].

Необхідно також згадати про міжнародну співпрацю на рівні приватних компаній. Такі технологічні гіганти, як Google та Facebook, запустили власні ініціативи для боротьби з фейковими новинами та маніпуляціями в Інтернеті. Вони використовують алгоритми для виявлення неправдивої інформації, а також співпрацюють із незалежними організаціями для перевірки фактів. Попри те, що ці компанії ще стикаються з багатьма викликами, їхня робота є важливим кроком на шляху до зниження впливу дезінформаційних кампаній на глобальному рівні.

Таким чином, успішні міжнародні ініціативи демонструють, що боротьба з дезінформацією можлива через комплексний підхід, що включає як державні, так і приватні заходи. Україна, аналізуючи ці приклади, може адаптувати кращі практики для подальшого посилення захисту свого інформаційного простору та підвищення стійкості суспільства до інформаційних загроз.

Висновки. Огляд наукових підходів до вивчення сутності інформаційної війни показав, що остання є невід'ємною складовою сучасної міжнародної політики. Вона використовується як засіб впливу на суспільну думку, державні структури та міжнародні відносини. Аналіз сучасних наукових розвідок дав змогу виявити, що інформаційні операції є складною комбінацією психологічних, технологічних та комунікаційних засобів, які спрямовані на дестабілізацію супротивника. Український досвід підтверджує важливість розуміння цих механізмів для ефективного протистояння інформаційним загрозам.

---

[18] Хакімова, В. Т. (2021). Європейський Союз в епоху постправди: діяльність East StratCom Task Force. *Актуальні проблеми політики.* Вип. 67. С. 155–162. DOI: https://doi.org/10.32837/app.v0i67.1166.

[19] Хорішко, Л. С. (2021). Досвід реалізації стратегічних комунікацій у діяльності НАТО та ЄС: інституційний аспект. *Регіональні студії.* № 26. С. 54–58. DOI: https://doi.org/10.32782/2663-6170/2021.26.11.

[20] Перемога над фейками. Як фінські учні опановують майстерність медіаграмотності (2020). *Нова українська школа.* [онлайн]. Режим доступу: https://nus.org.ua/articles/peremoga-nad-fejkamy-yak-finski-uchni-opanovuyut-majsternist-mediagramotnosti/(дата звернення: 03.10.2024).

Визначення ключових інструментів та технологій, що використовуються в інформаційній війні проти України засвідчило, що російська сторона активно застосовує широкий арсенал засобів, серед яких найбільш ефективними є дезінформація, пропаганда та кібероперації. Основними методами ведення інформаційної війни є поширення фейкових новин, маніпуляції наративами, інформаційні атаки на державні інституції та маніпуляція історичними фактами. Ці технології спрямовані на деморалізацію населення, послаблення довіри до влади та міжнародної підтримки України.

Безумовно, міжнародні ініціативи мають вагоме значення для підвищення рівня захисту інформаційного простору. Співпраця з Європейським Союзом, НАТО та іншими міжнародними організаціями сприяє посиленню інформаційної безпеки України, надаючи інструменти для боротьби з дезінформацією та підтримки стійкості до зовнішніх загроз. Успішні приклади міжнародних ініціатив, таких як East StratCom Task Force та NATO StratCom, можуть бути використані як основа для подальшого розвитку стратегій України у сфері інформаційної безпеки.

Список джерел

1. Білоусов, М. В., Алєйник, В. Г. (2023). Російська гібридна війна: загрози і кібервиклики для європейської інформаційної безпеки. *Регіональні студії.* № 33. С. 119–125. DOI https://doi.org/10.32782/2663-6170/2023.33.18.

2. Грицай, Р. О. (2023). Інформаційні війни: пошук стратегій протидії. *Публічне управління і адміністрування в Україні*. Вип. 33. С. 18–23. Режим доступу: https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf (дата звернення: 03.10.2024).

3. Галіпчак, В. (2023). Інформаційна війна як складова гібридної війни в умовах російської агресії. *Вісник Прикарпатського університету. Серія: Політологія.* № 15 (1). С. 26–32. DOI: https://doi.org/10.32782/2312-1815/2024-1-4.

4. Денисяка, О. (2024). Росія успішно просуває свої наративи про Україну у західних ЗМІ. *Голос Америки. Львівський портал*. [онлайн]. Режим доступу: https://portal.lviv.ua/news/2024/06/30/rosiia-uspishno-prosuvaie-svoi-naratyvy-pro-ukrainu-u-zakhidnykh-zmi-holos-ameryky (дата звернення: 03.10.2024).

5. Десять років з моменту трагедії рейсу MH17: пам'ять та правда (2024). *Електронне видання Еспресо*. [онлайн]. Режим доступу: https://espreso.tv/news-desyat-rokiv-z-momentu-tragedii-reysu-mh17-pamyat-ta-pravda (дата звернення: 03.10.2024).

6. Загурська-Антонюк, В. Ф. (2020). Політично-інформаційні безпекові механізми в українській державній системі у контексті геополітичних змін. *Державне управління: удосконалення та розвиток.* №2. Режим доступу: http://nbuv.gov.ua/UJRN/Duur_2020_2_10 (дата звернення: 03.10.2024).

7. Коріновська, Н., Грейс, М. (2017). Порошенко підписав указ про заборону «ВКонтакте» і Mail.ru в Україні. *Hromadske*. [онлайн]. Режим доступу: https://hromadske.ua/posts/prezydent-ukrainy-petro-poroshenko-pidpysav-ukaz-pro-novi-sanktsii (дата звернення: 03.10.2024).

8. Коруц, У. (2020). Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Підприємництво, господарство і право.* №8. DOI https://doi.org/10.32849/2663-5313/2020.8.55.

9. Краснодемська, І. Й. (2021). Окупація Криму Російською Федерацією в контексті геополітичної парадигми початку XXI ст. *Всеукраїнська науково-практичної конференція «Соціально-політичні процеси в Україні та світі у контексті глобалізаційних перетворень», 23 квітня 2021 року.* Ірпінь: Університет ДФС України. С. 81–90.

10. Сащук, Г. М., Рихлік, В. А. (2022). Інформаційний складник гібридної війни Росії проти України. *Політологічний вісник КНУ ім. Т. Шевченка.* № 89. С. 133–146. DOI: 10.17721/2415–88IX.2022.89.133-146.

11. Сопілко, І. М. (2022). Інформаційна війна проти України та правові засоби протидії злочинним засобам. *Юридичний вісник*. № 3 (64). С. 108–115. DOI: 10.18372/2307-9061.64.16897

12. Стадник, А. Г. (2015). Основні моделі організації інформаційних війн та їх різновиди. *Соціальні технології: актуальні проблеми теорії та практики.* Вип. 67–68. С. 81–91. Режим доступу: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf (дата звернення: 03.10.2024).

13. Тимошенко, Д. (2024). Від танків «з воєнторгу» до наступу на Київ: чому Захід 10 років боявся назвати РФ агресором. *Радіо Свобода.* [онлайн]. Режим доступу: https://www.radiosvoboda.org/a/viyna-rosiyi-proty-ukrayiny-vyznachennya/32826392.html (дата звернення: 03.10.2024).

14. Перемога над фейками. Як фінські учні опановують майстерність медіаграмотності (2020). *Нова українська школа.* [онлайн]. Режим доступу: https://nus.org.ua/articles/peremoga-nad-fejkamy-yak-finski-uchni-opanovuyut-majsternist-mediagramotnosti/ (дата звернення: 03.10. 2024).

15. Феськов, І. В. (2016). Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. *Актуальні проблеми політики.* Вип. 58. С. 66–77. Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/622a115c-5b8a-4cd3-8bf9-a87c614b3e66/content (дата звернення: 03.10.2024).

16. Хакімова, В. Т. (2021). Європейський Союз в епоху постправди: діяльність East StratCom Task Force. *Актуальні проблеми політики.* Вип. 67. С. 155–162. DOI: https://doi.org/10.32837/app.v0i67.1166.

17. Хорішко, Л. С. (2021). Досвід реалізації стратегічних комунікацій у діяльності НАТО та ЄС: інституційний аспект. *Регіональні студії.* № 26. С. 54–58. DOI: https://doi.org/10.32782/2663-6170/2021.26.11.

18. Kiera, J. (2022). Information warfare as a foreign policy tool of the russian federation. *No Limits*. Vol. 2. № 6. P. 30–31. DOI: https://doi.org/10.31261/no_limits.2022.6.09.

19. Stumbrus, V. (2024). Some elements of defining information warfare. *Public security and public order*. Vol. 35. P. 284–295. DOI: 10.13165/PSPO-24-35-21.

20. Szpyra, R. (2020). Russian information offensive in the international relations. *Security and Defence Quarterly*. Vol. 30. P. 31–47. DOI: http://doi.org/10.35467/sdq/124436.

References

1. Bilousov, M. V. and Alieinyk, V. H. (2023), “Rosiiska hibrydna viina: zahrozy i kibervyklyky dlia yevropeiskoi informatsiinoi bezpeky”, *Rehionalni studii*, No. 2, pp. 119–125, DOI https://doi.org/10.32782/2663-6170/2023.33.18.

2. Hrytsai, R. O. (2023), “Informatsiini viiny: poshuk stratehii protydii”, *Publichne upravlinnia i administruvannia v Ukraini*, Vol. 33, pp. 18–23, available at: https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf (accessed 03 October 2024).

3. Halipchak, V. (2023), “Informatsiina viina yak skladova hibrydnoi viiny v umovakh rosiiskoi ahresii”, *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia*, No. 15 (1), pp. 26–32, DOI: https://doi.org/10.32782/2312-1815/2024-1-4.

4. Denysiaka, O. (2024), “Rosiia uspishno prosuvaie svoi naratyvy pro Ukrainu u zakhidnykh ZMI”, *Holos Ameryky. Lvivskyi portal,* [онлайн], available at: https://portal.lviv.ua/news/2024/06/30/rosiia-uspishno-prosuvaie-svoi-naratyvy-pro-ukrainu-u-zakhidnykh-zmi-holos-ameryky (accessed 03 October 2024).

5. “Desiat rokiv z momentu trahedii reisu MH17: pamiat ta pravda” (2024), *Elektronne vydannia Espreso,* [онлайн], available at: https://espreso.tv/news-desyat-rokiv-z-momentu-tragedii-reysu-mh17-pamyat-ta-pravda (accessed 03 October 2024).

6. Zahurska-Antoniuk, V. F. (2020), “Politychno-informatsiini bezpekovi mekhanizmy v ukrainskii derzhavnii systemi u konteksti heopolitychnykh zmin”, *Derzhavne upravlinnia: udoskonalennia ta rozvytok,* No. 2. available at: http://nbuv.gov.ua/UJRN/Duur_2020_2_10 (accessed 03 October 2024).

7. Korinovska, N. and Hreis, M. (2017), “Poroshenko pidpysav ukaz pro zaboronu «VKontakte» i Mail.ru v Ukraini”, *Hromadske,* [онлайн], available at: https://hromadske.ua/posts/prezydent-ukrainy-petro-poroshenko-pidpysav-ukaz-pro-novi-sanktsii (accessed 03 October 2024).

8. Koruts, U. (2020), “Informatsiina viina yak instrument propahandy viiny: pravovi pidstavy protydii”, *Pidprymnytstvo, hospodarstvo i pravo,* No. 8, DOI https://doi.org/10.32849/2663-5313/2020.8.55.

9. Krasnodemska, I. I. (2021), “Okupatsiia Krymu Rosiiskoiu Federatsiieiu v konteksti heopolitychnoi paradyhmy pochatku XXI st., *Vseukrainska naukovo-praktychnoi konferentsiia “Sotsialno-politychni protsesy v Ukraini ta sviti u konteksti hlobalizatsiinykh peretvoren”, 23 kvitnia 2021 roku,* Irpin: Universytet DFS Ukrainy, pp. 81–90.

10. Sashchuk, H. M. and Rykhlik, V. A. (2022), "Informatsiinyi skladnyk hibrydnoi viiny Rosii proty Ukrainy", *Politolohichnyi visnyk KNU im. T. Shevchenka,* No. 89, pp. 133–146, DOI: 10.17721/2415–88IX.2022.89.133-146.

11. Sopilko, I. M. (2022), "Informatsiina viina proty Ukrainy ta pravovi zasoby protydii zlochynnym zasobam", *Yurydychnyi visnyk*, No. 3 (64), pp. 108–115, DOI: 10.18372/2307-9061.64.16897.

12. Stadnyk, A. H. (2015), "Osnovni modeli orhanizatsii informatsiinykh viin ta yikh riznovydy", *Sotsialni tekhnolohii: aktualni problemy teorii ta praktyky*, Vol. 67–68, pp. 81–91, available at: http://soctech-journal.kpu.zp.ua/archive/2015/67-68/11.pdf (accessed 03 October 2024).

13. Tymoshenko, D. (2024), "Vid tankiv "z voientorhu" do nastupu na Kyiv: chomu Zakhid 10 rokiv boiavsia nazvaty RF ahresorom", *Radio Svoboda,* [онлайн], available at: https://www.radiosvoboda.org/a/viyna-rosiyi-proty-ukrayiny-vyznachennya/32826392.html (accessed 03 October 2024).

14. "Peremoha nad feikamy. Yak finski uchni opanovuiut maisternist mediahramotnosti" (2020), *Nova ukrainska shkola,* [онлайн], available at: https://nus.org.ua/articles/peremoga-nad-fejkamy-yak-finski-uchni-opanovuyut-majsternist-mediagramotnosti/ (accessed 03 October 2024).

15. Feskov, I. V. (2016), "Osnovni metody vedennia hibrydnoi viiny v suchasnomu informatsiinomu suspilstvi", *Aktualni problemy polityky*, Vol. 58, pp. 66–77, available at: https://dspace.onua.edu.ua/server/api/core/bitstreams/622a115c-5b8a-4cd3-8bf9-a87c614b3e66/content (accessed 03 October 2024).

16. Khakimova, V. T. (2021), "Yevropeiskyi Soiuz v epokhu postpravdy: diialnist East StratCom Task Force", *Aktualni problemy polityky*, Vol. 67, pp. 155–162, DOI: https://doi.org/10.32837/app.v0i67.

17. Khorishko, L. S. (2021), "Dosvid realizatsi stratehichnykh komunikatsii u diialnosti NATO ta YeS: instytutsiinyi aspekt", *Rehionalni studii*, No. 26, pp. 54–58, DOI: https://doi.org/10.32782/2663-6170/2021.26.11.

18. Kiera, J. (2022), "Information warfare as a foreign policy tool of the russian federation", *No Limits*, Vol. 2, No. 6, pp. 30–31, DOI: https://doi.org/10.31261/no_limits.2022.6.09.

19. Stumbrus, V. (2024), "Some elements of defining information warfare", *Public security and public order*, Vol. 35, pp. 284–295, DOI: 10.13165/PSPO-24-35-21.

20. Szpyra, R. (2020), "Russian information offensive in the international relations", *Security and Defence Quarterly*, Vol. 30, pp. 31–47, DOI: http://doi.org/10.35467/sdq/124436.